최근 해킹 사고 분석 및 대비책 연구

강찬규, 최상명, 여돈구, 염흥열

순천향대학교 공과대학 정보보호학과

Analysis of Typical Hacking Attacks and Countermeasure to these Kinds of Attacks

ChanGyu Kang, SangMyung Choi, DonGu Yea, HeungYoul Youm

Department of Information Security Engineering, SoonChunHyang University

요 약

인터넷이라는 거대한 네트워크 망을 통해서 다양한 정보를 손쉽게 주고받을 수 있게 되었다. 하지만 대부분의 이용자들은 네트워크의 편리한 사용에만 관심을 두고 있으며, 보안에는 별로 신경을 쓰지 않고 있는 추세이다. 인터넷 이용자가 늘어남에 따라 정보들에 대한 보호의 필요성이 증가하고 있다. 보안은 개별 인터넷 이용자 시스템에서 시작하여 인터넷 서버 관리자 시스템까지 광범위하게 적용되어야 한다. 본 논문에서는 최근 유행하는 2가지 대표적인 해킹 사고의 예를 들어 원인을 분석하고 이를 방지하기 위한 대비책을 제시하며, 추후의 해킹 기술의 동향을 제시한다.

Ⅰ. 서론

초고속 인터넷의 보급과 네트워크의 전국적 보급으로 인한 인터넷 사용자(이하, 네티즌)의 급속한 증가는 정보이용의 효율성 증대라는 효과를 낳았다. 하지만 인터넷의 보급 속도에 미치지 못하는 네티즌과 관리자들의 보안 의식의 현주소는 매년 해킹 사고 급증이라는 부작용을 가져왔다.

새로운 해킹 기술의 고급화에 따라 관리자들의 보안 의식과 기술은 고급화가 요구되지만, 그렇지 못하고 있는 실정이다. 뿐만 아니라 관리자들의 미비한 대처에 따른 사고는 네티즌들의 피해로 이어지게 된다. 하지만 관리자들만의 노력으로 해킹 사고의 감소를 가져올 수는 없다. 무엇보다 중요한 것은 컴퓨터를 사용하는 네티즌들의 보안 의식 향상이다.

'03년 4월말 현재 KISA의 발표에 따르면 3310건의 해킹 사고가 접수되었다고 한다. 이는 전달 3400건에 비해 7%감소된 수치이다. 정부의 네티즌들에 대한 보안 의식 강화 정책에 따른 효과로 볼 수도 있을 것이다.

하지만 네티즌들의 보안 의식의 현주소는 기대수준에 못 미치고 있다. 그중 대표적인 것이 복잡한 패스워드의 사용과 OS(Operating System)의 패치 의 습관화와 백신의 설치가 미비하다는 점을 들 수 있다. 대부분의 네티즌들은 컴퓨터를 사용만 할뿐 관리에는 관심을 두지 않고 있어 자신의 정보가 노출되어있는지 조차도 알지도 못하는 경우가 많다.

Ⅱ장에서는 비 적합한 패스워드의 사용으로 인한 해킹 사례 및 관리자의 미비한 관리로 인한 해킹 사고 사례를 분석하고, Ⅲ장에서는 앞으로의 해킹 동향 및 대처방안을 제시한다.

Ⅱ. 본론

1. 000 해킹사건 분석.

사건발생 : 2003년 3월 24일 오후 5시 30분 ~ 6시 30분

가. 발생현상(추정)

: 192.168.000.000 (000.000.00.kr)에 해킹으로 인한 2차적 네트워크 스캔 공격에 의하여 많은 양의 packet이 대량 발생하여 네트웍 방화벽 처리 능력을 넘어 응답속도의 지연발생으로 인한 것임.

나. 해킹 사고 분석[1]

000의 인터넷접속을 끊은 후 실행프로세스 및 로그 확인. 피해 시스템 분석 전 하드 백업.

ps -aef 명령으로 먼저 어떠한 프로세스가 실행되고 있는 지 확인함. synscan이라는 많은 양의 프로세스가 백그라운드로 실행되고 있었음. find / -name synscan 으로 synscan의 위치 추적. jjingo 라는 user 의 home directory 내 숨겨진 디렉토리에서 발견.

jjingo user의 history 확인. 해커는 jjingo라는 계정으로 접속하여 wget 명령으로 여러 해킹 툴 및 exploit을 받아 root 권한을 획득하였음.

jjingo라는 계정으로 해커의 초기 접속 방법 조사. 당시 000서버는 3월 3일자로 처음 깔린 서버였다.

초기 해커의 유입경로는 last에서 보듯이

jjingo pts/0 66.78.00.00 Sat Mar 8 19:15 - 19:20 (00:04)

3월 8일이다. 3월 8일 동일 시간대의 로그를 살펴보았다. messeges 와 secure 에 의하면

- messeges.3

Mar 8 19:15:41 ramrec login(pam_unix)[22103]: authentication failure; logname= uid=0 euid=0 tty=pts/0 ruser= rhost=66.78.00.00 user=root

Mar 8 19:15:43 ramrec login[22103]: FAILED LOGIN 1 FROM 66.78.00.00 FOR root, Authentication failure

Mar 8 19:15:50 ramrec login(pam_unix)[22103]: session opened for user jjingo by (uid=0)

Mar 8 19:15:50 ramrec -- jjingo[22103]: LOGIN ON pts/0 BY jjingo FROM 66.78.00.00

- secure.3

Mar 8 19:15:32 ramrec xinetd[715]: START: telnet pid=22102 from=66.78.00.00

(추정)해커의 IP 66.78.00.00으로부터 한번의 root id로의 로그인 실패가 있은 후, jjingo라는 id로는 로그인 실패도 없이 바로 한번에 접속한 것을 알 수 있다. 이것으로 미루어 보아 이미 ramrec의 3월 3일 새로 리눅스를 설치하기 전에 이전 리눅스 서버에도 해킹을 시도하여 bruteforce어택 등으로 jjingo에 대한 계정으로의 접속을 시도하며 여러 번의 접속실패를 경험하며 패스워드를 알아냈을 가능성도 있다. (그러나 이는 정확히 추정하기 어렵다.)

가장 유력한 가능성은 jjingo 라는 userid는 password가 계정명과 동일하므로 해커가 jjingo라는 계정이 ramrec 서버에 있다는 것만 확인 할 수만 있었다면 아무 생각 없이 쉽게 jjingo/jjingo 이런 식으로 바로 접속을 했을 수도 있다.

- root history

jjingo

adduser -u 513 -g ramrec -d /home/ramrec/jjingo jjingo

passwd jjingo

jjingo라는 계정의 존재 여부는 쉽게 알 수 있었을 것이다. 이미 인터넷에 jjingo라는 계정이 ramrec에서 사용된다는 것을 알 수 있었다.

google등 검색엔진에서 jjingo라는 것을 쳐보면 jjingo라는 id에 관련된 서버의 도메인명이 나온다.

특히 jjingo 라는 userid를 쓰는 000 라는 사람의 홈페이지를 해커가 우연히 들르게 됐다고 가정하자 그 경우 jjingo의 홈페이지에는 다음과 같은 정보가 있다.

http://000.000/~jjingo/profile.html

이 름 : 0 0 0

E-Mail : jjingo@000.000.00.kr

위에서 보듯이 e-mail 부분에 jjingo@000.000.00.kr 이것을 보면 000서버에 jjingo라는 id가 존재함 을 알 수 있고 해커가 우연히 000에 접속하여 jjingo/jjingo 해서 접속했을 수도 있다. 해커의 초기 유입 동기는 확실하게 알 수 없지만 위에서 언급한 가정들로 접속했을 가능성이 매우 크다. jjingo라는 계정이 000에 있다는 것만 알더라도 브루트포스어택등 다양한 방법으로 접속을 시도 할 수 있었으나 특히 계정명과 패스워드가 동일했으므로 더욱 접속은 쉬웠을 것이다.

다. 대비책

위와 같은 취약점에서 보듯이 쉬운 암호는 쉽게 공격 당 할 수 있기 때문에 반드시 영문과 숫자 또는 특수기호를 혼합한 8자리 이상의 복잡한 패스워드를 사용하여야 한다.

2. 00나라 해킹사건 분석.

가. 발생현상

정보통신부는 사이버 공격에 관한 정보를 제공 하고 관련 사이트를 연결시켜주는 정보보호 포털 사이트(www.00.or.kr)를 개설, 4월 28일부터 일반에 제공했다.

28일 관련업계에 따르면 정보통신부의 정보보호 포털 사이트 "00나라"(www.00.or.kr)의 각종 정보를 담고 있는 데이터베이스에 접근할 수 있는 아이디와 패스워드가 손쉽게 일반에 노출됐다.

데이터 베이스 접근 아이디는 "kcve",패스워드는 "txxkcve"였다. 이 정보를 얻을 경우 "SQL 게이트"란 프로그램만 있으면 쉽게 데이터베이스 에 접속, 저장된 자료를 열람. 변조. 삭제할 수 있다.

특히 단순한 웹사이트 해킹이 아니라 데이터베이스 접근 권한이 노출됐기 때문에 정보보호와 관련된 정부 자료와 축적된 노하우가 순식간에 사라지거나 변질될 위험에 노출된 것으로 드러났다.

출처 : 한국경제 (2003.04.29)

데이터베이스 아이디와 패스워드는 몇 번의 클릭으로 손쉽게 얻을 수 있었다.

보호나라 웹사이트 초기화면의 "취약점DB"에 오른쪽 마우스를 클릭 하면 새 창이 떠워지고 이 창에 "http://211.000.000.000:8080/000/000/search.php"란 주소가 뜬다. .

이 주소 가운데 "search.php"를 삭제한 후 클릭 하면 여러 파일들이 보여지는데 여기서 "include/"와 "global.inc"를 순서대로 클릭 하면 인터넷 창에서 아이디와 패스워드를 볼 수 있다. 이 정도면 초보적인 해킹 지식만 있어도 손쉽게 아이디와 패스워드를 찾을 수 있다. 또한 데이터베이스의 아이디와 패스워드가 노출되면 이를 통해 얼마든지 해당 시스템에 들어가 자료를 마음대로 주무를 수 도 있다.

한 보안업체 관계자는 "아이디와 패스워드가 노출되면 웹사이트 해킹을 통해 자료접속 권한을 획득할 수 있어 얼마든지 데이터베이스 접속이 가능하다"고 말했다. 이에 대해 정보보호진흥원 관계자도 문제점을 인정했다.

이에 대해 한 보안업체 관계자는 "정부의 대표적인 보안 사이트가 노출됐다는 것만으로도 인터넷 강국이란 위상이 크게 흔들릴 수밖에 없다"고 지적했다.

나. 사건 재현

재현 서버 IP : 210.000.000.000

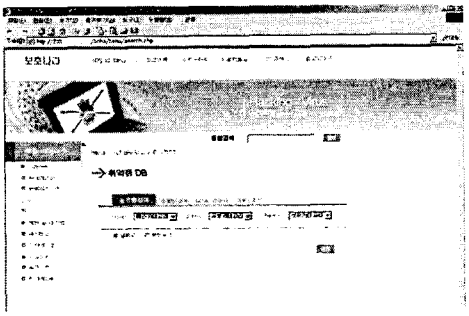

그림 1 :

http ://210.000.000.000/000/000/search.php

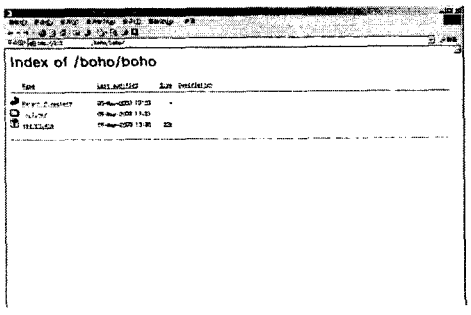

그림 2 :

http ://210.000.000.000/boho/boho/

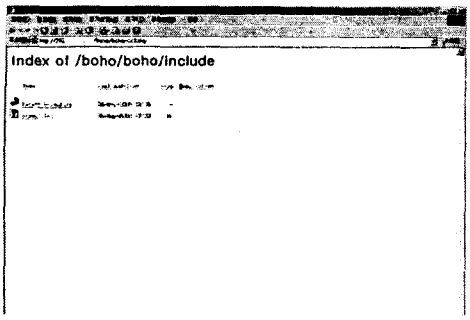

그림 3 :

http ://210.000.000.000/000/000/include/

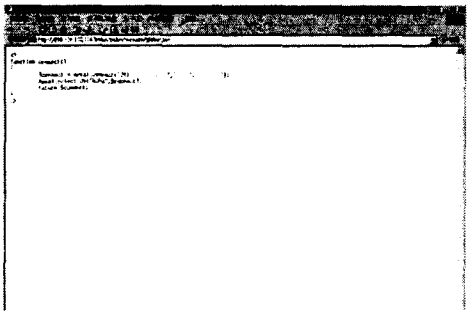

그림 4 :

http ://210.000.000.000/000/000/include/global.inc

다. 분석 및 해결책

보호나라 해킹 사건과 비슷한 경우의 .inc 환경설정파일의 취약점을 가진 사이트를 조사해 보았다. 상당히 많은 사이트들에서 이러한 문제점을 가지고 있음을 확인 할 수 있었다.

확장자가 .inc 의 파일에는 주로 db접속 계정명과 비밀번호를 담고 있기 때문에 해커에게 노출될 경우 db 정보의 열람 및 수정이 가능하여 매우 위험하다.

.inc 파일이란?

inclued 시키는 파일의 확장자를 많은 프로그래머들이 .inc로 저장을 하고 있다. 일종의 버릇을 이용한 해킹으로 프로그래머들이 .inc로 include시키는 버릇을 이용한 해킹 방법이다.

문제점은 웹사이트의 경로에서 .inc 파일의 경로를 알고 엑세스를 하게 되면 내용이 그대로 보여지게 된다는 점이다. 일반 텍스트파일이 브라우저에서는 내용이 나타나는 것과 같은 원리이다.

1) 확장자를 php로 사용할 것을 권장한다.

확장자가 php로 구성되어질 경우에는 웹 브라우저에 보여주기 전에 웹 서버에서 이미 PHP파일을 해석하고 브라우저로 보내게 되기 때문에 브라우저에 아무런 내용도 표시가 되질 않는다.

2) apache 환경 설정 파일(httpd.conf) 변경

apache[2] 환경 설정 파일(httpd.conf) 변경에 다음의 내용 추가 한다.

<Files *.inc>

Order allow,deny

Deny from al

</Files>

3) 브라우징 제거

아파치 의 디폴트세팅은 브라우징이 enable 되어 있다.

브라우징이란 웹브라우저에서 URL입력 시 index.html과 같은 정확한 파일명을 생략하고 디렉토리만 적었을 경우, 디렉토리 내 파일목록이 출력되는 현상을 말한다.

http.conf의 디렉토리 디렉티브내 다음줄 추가

Options -Indexes

라. 재현 해킹

저자들은 .inc 파일의 취약점을 이용한 해킹이 가능함을 보이고자 재현 서버를 구축 실제의 예를 들었다. 지금 여기에 보여지는 것은 저자들이 구축한 가상 서버이지만 실제로 이와 같은 서버들이 많이 존재한다는 것을 확인하였다. (이 웹 페이지는 가상의 웹 페이지임을 알려준다.)

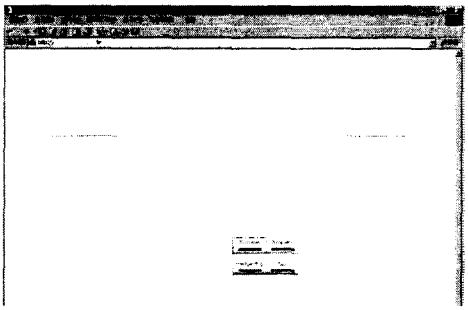

그림 5 : 웹페이지 접속

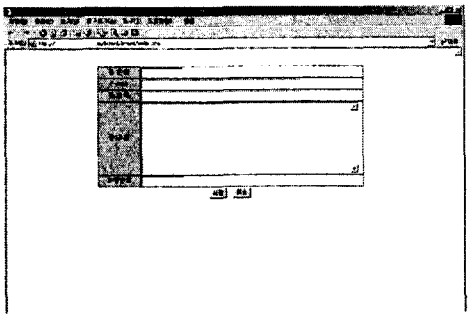

그림 6 : 게시판 접속

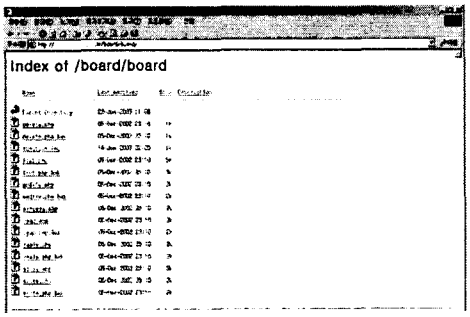

그림 7 : write.php제거

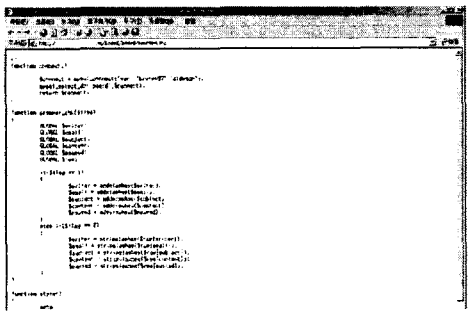

그림 8 : function.inc 접속

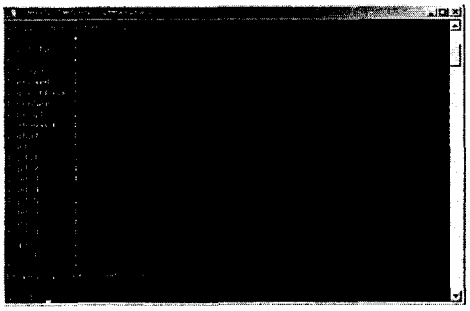

그림 9 : db 접속

지금까지 살펴본 바와 같이 해킹은 정말 사소한 것에서 발생할 수가 있다. 앞에서 본 것처럼 해커가 쉽게 로컬 접속을 할 수 있으며 로컬 접속 후 2차 로컬어택 을 시도하여 root 권한을 획득하는 것은 그리 어렵지가 않을 것이다.

.inc 환경설정파일은 include라는 기능을 이용하여 서버관리자(또는 웹서버관리자)에게 편리함을 주지만 그 기능은 해커들에게는 좋은 표적이 될 수 있는 것이다. 관리자는 .inc 파일을 .inc.php 처럼 php 확장자 또는 asp 등으로 바꾸어 주어 해커가 볼 수 없도록 또는 아파치 환경설정 파일을 수정하여 .inc파일을 외부사람이 볼 수 없도록 해야 할 것이다.

Ⅱ. 결론

요즘 들어 해킹 기술이 날로 지능화 되고 고도화되고 있다. 기존의 해커들이 사용했던 exploit의 사용법이 더욱 간단해지고 더욱 강력해졌다. 단지 exploit의 실행만으로 root를 획득 할 수 있는 것이다. 게다가 요즘의 exploit은 큰 IP 클래스를 상대로 스캔을 하여 해당 취약점이 있는 서버를 공격하기 때문에 한번에 많은 컴퓨터를 해킹 할 수 있다. 또한 취약점과 웜이 합쳐져 순식간에 모든 네트워크가 감염될 수 있다.

최근에는 공유폴더[3] 취약점의 문제도 심각하다. 공유폴더의 취약점으로 인해 커다란 보안사고가 많이 발생하고 있다. 공유폴더는 외부에서 접근이 가능하게 공유를 시켜놓은 폴더를 말한다. 윈도우 환경에서의 공유폴더는 사용자들에게 파일을 서로 공유하기 쉽도록 해주는 장점이 있기 때문에 유용한 방법이기는 하나, 이러한 공유폴더에는 취약점이 있다. 암호를 걸지 않은 공유 폴더는 누구든지 접근이 가능하며 이렇게 접근이 가능한 공유 폴더에는 바이러스 및 해킹의 위험성이 많이 내포되어 있다.

특히 사용자들이 많이 쓰는 Windows 2000/XP 환경에서의 기본적으로 관리되는 공유 폴더는 Administrator의 암호를 걸지 않게 되면 IP를 알 경우 누구나 쉽게 접근 가능하며, 공유폴더를 통해 바이러스의 유포 및 해킹이 가능하다. 이러한 문제점의 해결책으로는 Administrator의 암호를 반드시 걸어주고, 쉬운 암호는 쉽게 공격 당 할 수 있기 때문에 반드시 영문과 숫자 또는 특수기호를 사용한 8자리 이상의 복잡한 패스워드를 사용하여야 한다. 또한 OS에 대한 패치도 꾸준히 하며 백신도구를 사용하여 바이러스 에 대한 감시도 철저히 하여야할 것이다.

이처럼 앞으로의 해킹은 더욱 빠르고 대량으로 확산되기 때문에 사용자 및 관리자의 주의가 필요하다. 관리자는 자주 CERTCC 등 여러 보안 사이트에서 발표하는 취약점 을 참고하고 자신의 서버의 취약점을 즉시 패치 한다. 또한 간단한 security tool등을 사용하여 미연에 해킹을 방지하는 노력이 필요하다고 볼 수 있겠다.

해킹 피해 시스템 분석 후 앞으로 관리자가 해야 할 일은 여러 가지가 있을 수 있지만 먼저 해당 취약점을 찾아서 이를 막는 것이 급선무이다. 또한 해당 데몬 또는 프로그램에 대한 최신 보안 패치를 받아 설치한다. 그리고 서비스 돼고 있지 않은 포트를 확인하여 막고 방화벽 또는 IDS를 설치하여 다음의 공격으로부터 미리 방어기지를 구축해 놓아야 한다고 할 수 있다. 또한 로그의 변조 등을 막기 위하여 다른 서버로의 로그를 백업할 수 있도록 한다. 각종 보안 툴 의 설치도 좋은 방법 중의 하나 일 것이다. 본 논문에서 제시된 두 가지 해킹 기법은 매우 일반화된 해킹 기법으로써, 이를 막기 위한 관리적 대책이 시급히 요구된다.

참고문헌

[1] 유닉스 로그분석을 통한 침입자추적 및 로그 관리 Part1
http://www.certcc.or.kr/paper/tr2001/tr2001-05/unix_log_analysis.pdf

[2] Apache 웹서버 보안관리
http://www.certcc.or.kr/paper/tr2002/tr2002_10/apache_Security.pdf

[3] [기술문서] 윈도우즈 환경에서의 공유폴더 취약점을 이용한 공격유형 및 취약점 대응방법
http://www.certcc.or.kr/paper/tr2003/030423.pdf